CLAIMS:

1. A method for defence against at least one attack made by means of differential power analysis in at least one hyperelliptic cryptosystem, in particular in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve (C) of any genus (g) over a finite field (K) in a first group, where the hyperelliptic curve (C) is given by at least one co-efficient, characterised in that the hyperelliptic curve (C) and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication is randomised.

2. A method as claimed in claim 1, characterised in that the bits of the operand to be processed and/or encoded in the hyperelliptic cryptosystem are represented by the hyperelliptic curve (C), in particular by at least one co-efficient of the hyperelliptic curve (C), and/or by at least one base element of the cryptosystem, such as by at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication.

3. A method as claimed in claim 1 or 2, characterised in that at least one scalar multiplication in the Jacobian variation $J(C)$(K) of the hyperelliptic curve (C) takes place in a second group different from the first group and isomorphic in relation to the first group, in particular selected at random.

4. A method as claimed in claim 3, characterised by the following steps:

- transformation of the Jacobian variation $J(C)$(K) of the hyperelliptic curve (C) by means of at least one depiction (ϕ), in particular by means of at least one K-isomorphism, into the Jacobian variation $J(\tilde{C})$(K) of the transformed hyperelliptic curve ($\tilde{C} = \phi(C)$);
- multiplication of the Jacobian variation $J(\tilde{C})$(K) of the transformed hyperelliptic curve ($\tilde{C}$) with at least one scalar (n); and
- back transformation of the Jacobian variation $J(\tilde{C})$(K) multiplied by the scalar (n) of the transformed hyperelliptic curve ($\tilde{C}$) by means of the depiction (ϕ^{-1}) inverse to

the depiction (ϕ) in a Jacobian variation $J(C)$ of the hyperelliptic curve (C) multiplied by scalar (n),

- where

-- the depiction (ϕ) corresponds to the transition from the first group to the second group

-- the inverse depiction (ϕ^{-1}) corresponds to the transition from the second group to the first group.

5. A method as claimed in at least one of claims 1 to 4, characterised by the following steps:

- depiction of at least one in particular reduced divisor (D) with associated polynomial pair as at least one quintuplet $[U_1, U_0, V_1, V_0, Z]$ in projective co-ordinates, where $U(t) = t^2 + U_1t/Z + U_0/Z$ and $V(t) = V_1t/Z + V_0/Z$;

- selection, in particular random selection, of at least one non-vanishing element (s) from the field (K^x); and

- conversion of the quintuplet $[U_1, U_0, V_1, V_0, Z]$ by means of a selected element (s) into the converted quintuplet $[sU_1, sU_0, sV_1, sV_0, sZ]$.

6. A method as claimed in at least one of claims 1 to 4, characterised by the following steps:

- depiction of at least one in particular reduced divisor (D) with associated polynomial pair as at least one sextuplet $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ in projective co-ordinates, where $U(t) = t^2 + U_1t/Z_1^2 + U_0/Z_1^2$ and $V(t) = V_1t/(Z_1^3Z_2) + V_0/(Z_1^3Z_2)$;

- selection, in particular random selection, of at least two non-vanishing elements

(s_1, s_2) from the field (K^x); and

- conversion of the sextuplet $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ by means of a selected elements

(s_1, s_2) into the converted sextuplet $[s_1^2U_1, s_1^2U_0, s_1^3s_2V_1, s_1^3s_2V_0, s_1Z_1, s_2Z_2]$.

7. A method as claimed in any of at least one of claims 1 to 6, characterised in that the method is implemented on at least one microprocessor in particular allocated to at least one chip card and/or in particular to at least one smart card.

8. A microprocessor working according to a method as claimed in at least one of claims 1 to 7.

9. A device, in particular a chip card and/or in particular a smart card, with at least one microprocessor as claimed in claim 8.

10. Use of a method as claimed in at least one of claims 1 to 7 and/or at least one microprocessor as claimed in claim 8 and/or at least one device in particular at least one chip card and/or at least one smart card as claimed in claim 9 in the defence against at least one attack made by means of differential power analysis on at least one hyperelliptic cryptosystem, in particular at least one public key cryptosystem.